

AUSA: Trevor Broad

Telephone: (313) 226-0210

AO 106 (Rev. 04/10) Application for a Search Warrant Special Agent:

Julia MacBeth (FBI)

Telephone: (313) 919-1373

UNITED STATES DISTRICT COURT

for the
Eastern District of MichiganIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)44135 Trent Dr., Clinton Township, Michigan 48038
(More fully described in Attachment A)

Case No. 23-mc-50730-4

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §1349

Conspiracy to Commit Wire Fraud

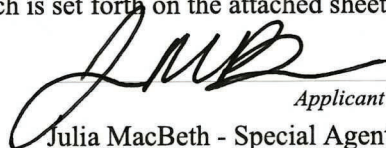
18 U.S.C. §§ 1343 & 1344

Wire fraud & Bank Fraud

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

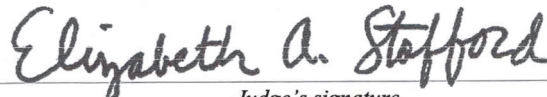


Applicant's signature

Julia MacBeth - Special Agent - FBI

Printed name and title

Sworn to before me and signed in my presence
and/or by reliable electronic means.

Date: June 22, 2023City and state: Detroit, Michigan


Judge's signature

Hon. Elizabeth A. Stafford U. S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Julia MacBeth, Special Agent for the Federal Bureau of Investigation,
being duly sworn, state as follows:

INTRODUCTION

1. There is probable cause to believe that XAVIER HICKS, a resident of the Eastern District of Michigan, is part of a conspiracy and a participant in an ongoing fraudulent scheme that is defrauding credit unions by impersonating credit union members and fraudulently withdrawing funds from the impersonated members' accounts. Probable cause exists that evidence, instrumentalities and fruits of this conspiracy and fraudulent scheme are located at HICKS's residence in the Eastern District of Michigan.

2. Accordingly, I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search HICKS's residence, located at 44135 Trent Dr., Clinton Township, Michigan 48038, hereinafter the "SUBJECT RESIDENCE," further described in Attachment A, for the items described in Attachment B, which are items that constitute evidence, instrumentalities, and/or fruits of violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft), collectively, the SUBJECT OFFENSES. I am requesting authority to search the

entire premises (including any sheds or garages, and any safes or locked storage containers) and any vehicles, computers (to include cellular devices) or computer storage media located therein where any of the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of the SUBJECT OFFENSES.

AFFIANT BACKGROUND

3. I am a Special Agent of the FBI and, as such, an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. I am empowered to conduct investigations of and to make arrests for offenses enumerated in Title 18 of the United States Code.

4. I have been employed by the FBI since May 2016. Prior to joining the FBI, I was a Federal Air Marshal from December 2010 until April 2016. I have received law enforcement training at the Federal Law Enforcement Training Center (FLETC) and the FBI Academy. During my employment with the FBI, I have investigated federal crimes involving mail fraud, wire fraud, bank fraud, money laundering, investment fraud, identity theft, and various other criminal matters. At all times during the investigation described in this affidavit, I have been acting in an official capacity as a Special Agent of the FBI.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and

witnesses. This affidavit is submitted for the limited purpose of showing that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

SUMMARY

6. Beginning at least in May 2022 and continuing to the present, XAVIER HICKS and other co-conspirators are conspiring and participating in a scheme to defraud credit unions by impersonating credit union members and fraudulently withdrawing funds from the impersonated credit union members' accounts. The impersonated victims are typically employees or board members of the credit union. In addition, investigators have uncovered evidence that HICKS has used victims' credit cards without their consent. The loss amount is believed to be in the hundreds of thousands of dollars.

7. Multiple sources of evidence connect HICKS to the SUBJECT OFFENSES and support probable cause to believe that HICKS is an active participant in the SUBJECT OFFENSES. Investigators have identified phone numbers used to perpetrate the fraud on the credit unions that were also used during the same period to commit credit card fraud to purchase goods and services in HICKS's name. Historical location records for one such phone number came back to the area of HICKS's known residence, *i.e.*, the SUBJECT RESIDENCE.

And, another phone number that was used to contact credit unions prior to their victimization was registered in HICKS's name.

8. In addition, I have heard recordings of calls to credit unions by a perpetrator in this fraudulent scheme and believe the voice on those calls sounds consistent with the voice I have heard in recordings on HICKS's personal social media page, which leads me to believe that the caller/perpetrator is HICKS. Further, call records show frequent calls between HICKS and co-conspirators who are known to travel to the credit unions and recruit individuals to go in to make withdrawals. This evidence supports investigators' belief that HICKS calls into credit unions and uses victims' personal identifying information to fraudulently request that funds be transferred out of the victims' accounts.

9. In furtherance of this scheme to defraud, probable cause exists that HICKS has: used interstate electronic communications to contact victimized credit unions and communicate with co-conspirators; caused interstate wire communications by credit unions and/or financial institutions; and possessed and used victims' personal identifying information (PII) and/or a means of identification of another person without lawful authority.

10. Finally, HICKS has a prior federal conviction for conspiring to commit bank fraud, which further supports probable cause to believe that HICKS is involved in the SUBJECT OFFENSES, which are fraud related offenses.

PROBABLE CAUSE

11. In 2014, HICKS was arrested and convicted of violating 18 U.S.C. § 1344 (Conspiracy to Commit Bank Fraud). The prior FBI investigation into HICKS identified HICKS as the leader of a ring conducting account takeovers of Bank of America accounts, a very similar scheme as the one detailed in this affidavit. HICKS was sentenced to 96 months' imprisonment and ordered to pay \$1.7 million in restitution. HICKS was released from federal custody in 2021 and is currently on supervised release. As noted above, his prior conviction supports probable cause to believe that he is involved in the SUBJECT OFFENSES, which are fraud-related offenses that appear to have begun in the period after HICKS was released from custody and involve a similar scheme to the one for which he was convicted.

12. In December 2022, the FBI began investigating a potential account takeover ring that was targeting credit unions after the FBI received multiple local police reports and complaints from credit unions, many located in the Eastern District of Michigan, detailing the same type of fraudulent account takeover activity.

13. The reported fraud scheme involved suspects obtaining PII of members of credit unions that are partnered with Co-op Credit Solutions and participate in a shared branch network. The Co-op shared branch network allows

members of a credit union to perform a range of transactions at another credit union within the network. The reports indicated that the suspects would call into the Co-op Solutions automated call center to obtain account details of a victim's account. The suspects then would recruit an impersonator go into a different credit union within the co-op network to withdraw money from the victim's account. To make the withdraw, the impersonator presented a fictitious driver's license in the victim's name. Several impersonators (also known as "mules") were observed on surveillance video at other locations where this fraud occurred. This fraud is also known as "shared banking fraud." The victims most often targeted in this scheme are employees or board members of the credit union.

14. This fraud ring has also recently targeted credit unions not within the co-op network. In these instances, individuals are recruited to open accounts at credit unions. The suspects then call into credit union call centers, impersonating members to cause a wire transfer from the member's accounts to the newly established accounts. The suspects then pay the recruited individuals to go into branches to withdraw the money which was transferred into the new accounts or use a debit card connected with the account to deplete the funds.

15. I know from other investigations and from conversations with other agents who have investigated shared banking fraud schemes that perpetrators can obtain the PII of victims through a variety of sources. One source perpetrators

frequently use is public social media sites, such as the employment focused site LinkedIn. LinkedIn can be used to identify employees and board members of credit unions. Additionally, PII for these employees can be obtained on the dark web. I know that perpetrators access the dark web using personal computers and other electronic devices with internet access in the privacy of their home, and that evidence of how the perpetrators obtained the PII can be found on their electronic devices in their home. PII that can be found on the dark web includes financial institution account numbers, address history, telephone numbers, and names of relatives.

16. This fraud scheme is active and instances of this ring committing this fraud have been reported to the FBI as recent May 2023.

17. Based off information provided by the victimized credit unions, numerous phone numbers have been identified as being used to call into the call centers to cause the wire transfers or to gain account information. Call records and subscriber information for these identified numbers indicate the numbers were established and used for short durations for the purpose to commit this fraud. The

call records show calls made to credit unions, banks, credit card companies, and identified co-conspirators.

Capital One

18. A review of T-Mobile records for numbers such as 734-***-9452 and 865-***-7754, which were used to contact credit unions in this fraud, referenced in greater detail below, also showed multiple contacts to Capital One Bank. A list of identified numbers used to call the credit unions in furtherance of this fraud were provided to Capital One for review.

19. Capital One Bank provided a report of all contacts the above phone numbers made to Capital One. The identified phone numbers were used to call into Capital One to dispute declined charges or get transaction updates on at least 36 different compromised credit card accounts. Many of the successful fraudulent charges resulted in a loss to the merchant.

20. Some of the fraudulent charges resulted in the merchant filing a dispute. One such dispute was from a trucking company in Sterling Heights, where a stolen Capital One credit card number had been used for a payment of \$22,310.45 in semi-truck repairs. The receipt provided by the trucking company showed the client who had use the stolen card number was HICKS.

21. Three more charges, totaling \$9,748.47, were made at Progressive Insurance for payments on an insurance policy. Records provided by Progressive

Insurance showed the account associated with the fraudulent transactions was for an insurance policy for semi-trucks owned by HICKS. HICKS's public social media pages often display information about his logistics business, HXL Freight Systems. According to the Michigan Department of Licensing and Regulatory Affairs, HXL Freight Systems was registered by JDESRAY HICKS (HICKS's wife), with the SUBJECT RESIDENCE listed as the business address. The SUBJECT RESIDENCE is a single-family residence, not a commercial location.

22. In January 2023, the phone number 734-***-9452 was used to call into Sun Federal Credit Union in Ohio to impersonate members and defraud Sun Federal out of \$6,495. The same number was used by a male-sounding voice multiple times in December 2022 to call into Capital One concerning a credit card opened in the name of JDESRAY HICKS (HICKS's wife) which was registered to the SUBJECT RESIDENCE.

23. Of these transactions, at least \$13,736 in attempted charges were made using the stolen credit cards numbers at a Detroit area merchant, Dessy & Co, Inc. According to the Michigan Department of Licensing and Regulatory Affairs, Dessy & Co LLC was organized in 2020 by JDESRAY HICKS, the wife of XAVIER HICKS. The website, www.dessyandco.com, states that Dessy & Co was founded by JDESRAY HICKS of Detroit, MI. Therefore, if HICKS were making charges with stolen credit cards at his wife's company and there were no

goods exchanged, HICKS' wife, JDESRAY, would receive a fraudulent payout from Capital One with no expense to the company.

24. Capital One provided recordings of some of the phone calls by the above-identified phone numbers. I have listened to these calls and based on my review, the male sounding voice in these recordings, sounds to me like the voice in recordings of conversations with the credit union employee impersonators, which were provided by a Co-Op Solutions call centers. In multiple instances, it sounded to me like the caller attempted to make his (male) voice sound like a female when impersonating female credit union members. I believe the same caller was making these calls, and that the caller is HICKS.

Liberty Federal Credit Union

25. According to reports provided by Liberty Federal Credit Union (LFCU) and the Murfreesboro (Tennessee) Police Department, on February 24, 2023, LFCU received a large volume of calls from someone impersonating credit union members requesting money transfers from their accounts to newly established accounts at LFCU. One of the identified phone numbers used to call into LFCU was 865-***-7754.

26. The suspect calling from phone number ending 7754 had personal identifying information of a victim, including the victim's social security number

and the name of the joint owner on the victim's account. With this information, the suspect was able to transfer \$8,500 into another account to be withdrawn.

27. T-Mobile phone records for the number ending 7754 showed that this number contacted LFCU twice on February 24, 2023, the day the victim's money was transferred out of their accounts, once at 22:47 and once at 22:57 Coordinated Universal Time (5:47 PM and 5:57 PM Eastern Standard Time). Historical location records provide by T-Mobile indicate that the phone using the number ending 7754 was in the area of the SUBJECT RESIDENCE.

28. Historical cell tower location information for the number ending 7754 indicates during these call times the cell tower pinged by the number ending 7754 was located within the area of the SUBJECT RESIDENCE. Additionally, timing advance records collected by T-Mobile provided multiple GPS coordinates during this calling period for voice and data location records, which all place the phone using the number ending 7754 number within close proximity to the SUBJECT RESIDENCE.

29. Based on my training and expertise of my associates, I know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of cellular devices to which they provide service. That information includes (1) cell-site data, also known as "tower/face information" or cell tower/sector records and (2) timing advance or

engineering data commonly referred to as per call measurement data. Data such as timing advance records, provide relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas.

30. In other instances of the credit union fraud, the review of detailed phone records between the phone number ending 7754 and other identified co-conspirators, as referenced below, show a series of calls where phone records for HICKS show calls into credit unions then immediately calls to a known recruiter who travels out to the area of the targeted credit union.

31. The co-conspirators, as referenced above, were identified through physical surveillance, license plate recognition (LPR) cameras, and images obtained from credit union closed circuit television cameras (CCTV). The co-conspirators roles in this scheme were to drive mules to the credit union to withdraw money, or to recruit people to open accounts with the intent to transfer funds into the accounts. One such co-conspirator, was observed driving a rental

car, which was observed via LPRs and CCTV at the scene of multiple credit unions where the fraud described in this affidavit occurred.

Triboro Federal Credit Union

32. On January 31, 2023, the CEO of TriBoro Federal Credit Union, located in Pennsylvania, contacted the FBI to report a series of fraud incidents that the credit union had experienced in the days prior. The CEO stated that on January 25 and 26, 2023 an unidentified woman made withdraws on three different TriBoro employees' accounts at various shared banking branches in Louisiana. The co-op call center which handles the mobile banking for TriBoro reported that a few phone numbers had called into the call center about those accounts in the days leading up to the fraud in attempts to gain information about the victims' accounts.

33. One of the phone numbers that called into the co-op call center about one or more of the victims' accounts in the days leading up to the fraud was 586-***-9497. Specifically, on January 21, 2023, four days prior to the fraudulent withdraws, 586-***-9497, contacted the TriBoro call center. According to law enforcement database checks, and confirmed by records provided by T-Mobile, phone number ending 9497 was registered to HICKS.

34. As part of his federal supervised release, HICKS was required to fill out a financial disclosure form and identify all financial institutions where he banked. HICKS did not list TriBoro Credit Union as a location where he has an

account. Accordingly, investigators believe that HICKS's contact with the TriBoro call center was in furtherance of the SUBJECT OFFENSES.

HICKS's Facebook Account

35. An open-source database check revealed a public Facebook account in the name "XAVIER HICKS." The pictures posted to the account match the driver's license photo of HICKS. Additionally, friends associated with this account include HICKS' wife, JDESRAY HICKS. Based on this information, I believe the Facebook account belongs to HICKS.

36. On May 3, 2023, HICKS posted a live video to his Facebook page titled "...At the house office after hours." In the hour-long video, HICKS can be seen singing and discussing making money with another person. HICKS states that he has spent the day working from home. At one point a stack of money was thrown on the table. Binders, documents, computers and filing cabinets can be observed in the background of the video.

37. In the same live video, HICKS also stated that they just received a Door Dash delivery of alcohol. Records obtained from Door Dash confirmed an order from Harbors Market on May 3, 2023, placed in the name of HICKS that was delivered to the SUBJECT RESIDENCE.

38. Based on the information from his Facebook account, the Facebook video, and Door Dash records, investigators believe that the live video was taken at

the SUBJECT RESIDENCE, that HICKS conducts his fraudulent activities at the SUBJECT RESIDENCE, which is what he was referring to when he said he was working from home, and that evidence (such as the documents and binders in the video), instrumentalities (such as computer in the video) and fruits (such as the stack of cash in the video) of his fraudulent activities and the SUBJECT OFFENSES are at the SUBJECT RESIDENCE.

SUBJECT RESIDENCE

39. According to the Macomb County Register of Deeds, JDESRAY HICKS purchased the SUBJECT RESIDENCE on April 12, 2022.

40. In February 2023, HICKS changed his address with the Secretary of State to the SUBJECT RESIDENCE. On June 2, 2023, HICKS was observed driving a Cadillac Escalade, registered to him, in front of the SUBJECT RESIDENCE.

41. On June 9, 2023, HICKS's federal probation officer visited HICKS at the SUBJECT RESIDENCE to remove HICKS's electronic monitoring device.

42. As a term of his federal supervised release, HICKS is prohibited from traveling outside the State of Michigan without prior approval. Based on these restrictions, it is likely that HICKS made the calls to the credit unions in furtherance of the SUBJECT OFFENSES, as discussed above, from the SUBJECT RESIDENCE and in the local area, which is in the Eastern District of Michigan.

43. Based on my training and experience, and from information received from other law enforcement officers, I am aware that persons who engage in fraud and identity theft rely on computers and mobile electronic technology to commit these criminal offenses. Such individuals often create and maintain records of the fraudulent activities on computers, tablets, cell phones, and portable electronic media, such as portable thumb drives and external hard drives. Such information typically includes correspondence and memos, receipts, telephone records, bank, credit/debit card account and financial information, notes and personal documents, template card and identification images, and the names of co-conspirators, if any. This information is often stored in electronic or magnetic form. Such devices are often stored at a person's residence and home office.

44. Based on my training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" files on a computer, the data contained in the file does not actually disappear; rather the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space; that is, in space on the hard

drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. Due to the size of storage systems on modern computers—often 500 gigabytes or greater—deleted files are rarely overwritten by new data.

45. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

46. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted or password protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in laptop computers. Consequently, each computer found during a search can easily contain the equivalent of 80 million pages of data.
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly

unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

47. In light of these concerns, I hereby request the Court’s permission to transport the seized items to the FBI Detroit Field Office or other law enforcement locations to search, copy, and image the computer/mobile electronic hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an offsite search of the image or hardware for the evidence described.

48. I also know, based upon my training, knowledge, and experience, that persons engaged in the above activities frequently have large amounts of U.S. currency, which are the proceeds of the crime, in secure places such as safes, storage units and lock boxes. For this reason, I am requesting that if any safes or other locked containers are found on the premises, locksmiths may be used to open the safe or container either on the premises, or if reasonably necessary, any safe or container may be moved off-premises to be opened.

49. Based on my training and experience, I know that individuals involved in the use of fraudulent access devices often maintain records relating to their criminal activity. These records are often maintained in various forms ranging from printed business and bank records, to handwritten notations on pieces of paper, to notebooks, to ATM receipts, to computer stored and generated records. Based on my training, experience, and discussions with other law enforcement officers, I know that individuals who engage in fraudulent activities, including the manufacturing and passing of counterfeit access devices, and fraudulent identification documents often maintain historical books, records, receipts, notes, ledgers, and copies of checks or other financial instruments used to facilitate the scheme to defraud. These individuals normally keep these records in their residences and/or vehicles where they can readily have access to them. For these reasons, I am requesting permission to search for and seize such items from the locations described in Attachment A.

50. Further, as noted above, HICKS is currently on federal supervised release and his federal probation officer has visited the SUBJECT RESIDENCE. Based on my training and experience, I know that those who are on parole or supervised release and who are engaged in criminal activities, including financial fraud like that described in this affidavit, will keep records in their residence, like the SUBJECT RESIDENCE despite being on parole or supervised release, but may

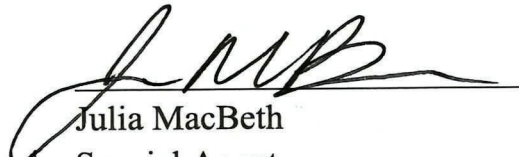
take extra steps to try to hide or conceal the evidence from plain view because they know a parole officer may make a home visit. For instance, a criminal may try to hide records in places not easily seen, such as in a garage, or in the trunk of a vehicle that is inside a garage or shed. Accordingly, as noted above, I am requesting that the search warrant authorize a search of the entire premises (including any sheds or garages, and any safes or locked storage containers) and any vehicles on the premises.

CONCLUSION

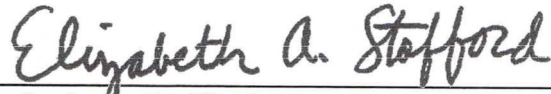
51. Based on the information contained herein, there is probable cause to believe that the SUBJECT RESIDENCE, further described in Attachment A, will contain items described in Attachment B, which constitute evidence, fruits, and instrumentalities of the SUBJECT OFFENSES.

52. I submit that this affidavit supports probable cause for a warrant to search the residence described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,


Julia MacBeth
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence
and/or by reliable electronic means.

A handwritten signature in cursive script that reads "Elizabeth A. Stafford". The signature is written in dark ink and is positioned above a horizontal line.

Elizabeth A. Stafford

United States Magistrate Judge

Attachment A

DESCRIPTION OF SUBJECT RESIDENCE TO BE SEARCHED

A two-story light brick house with basement, light grey roof located at 44135 Trent Dr, Clinton Township, MI 48038. The house has two brown glass doors that face east toward Trent Drive. The house number is next to the front door. The premises is further defined to include any garages or sheds and any safes or locked storage containers, as well as any vehicles parked at the premises, and all computers (to include cellular devices) or electronic storage media.



ATTACHMENT B

All evidence, fruits and instrumentalities relating to violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft), including:

1. Any items, materials, documents, communications, and/or records, in whatever form, relating to the personal identifying information of victims, to include but not limited to, names, social security account numbers, addresses, dates of birth, bank statements, credit cards, debit cards, identification documents, handwritten notes, and other miscellaneous documents.
2. Any items, materials, documents, communications, and/or records, in whatever form, referencing, regarding or relating to producing identification cards, including but not limited to drivers' licenses.
3. Any items, materials, documents, communications, and/or records, in whatever form, referencing, regarding or relating to the use of credit and debit cards.
4. Any items used to create counterfeit access devices or identity documents, including, but not limited to plastic card stock, printers, reader/writers, and embossers.

5. Items, materials, documents, communications, and/or records, in whatever form, relating to the ownership, occupancy, or use of the premises to be searched.

6. Any cash; or items, materials, documents, communications, and/or records, in whatever form, identifying the location of safety deposit boxes, storage units, or other possible depositories for cash; and other liquid assets which are identified in any way with XAVIER or JDESRAY HICKS, or known aliases, such Marvin Nicholson, and/or business entities owned by XAVIER or JDESRAY HICKS, and any keys or other access devices associated with such depositories.

7. Any safes or other locked containers which could contain any of the above. If any safes or other locked containers are found on the premises, locksmiths are to be used to open the safe or container either on the premises, or if reasonably necessary, any safe container may be moved off-premises to be opened.

8. Any items, materials, documents, communications, and/or records, in whatever form, evidencing receipt, location, or disposition of assets and proceeds derived from identity theft, or bank fraud.

9. Any items, materials, documents, communications, and/or records, in whatever form, which contain the identity of other associates or the identity of co-conspirators.

10. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant.

- a. For any computer hard drive or other electronic media (hereinafter, “MEDIA”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:
 - i. Evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;
 - ii. Passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
 - iii. Documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

AUSA: Trevor Broad

Telephone: (313) 226-0210

AO 93 (Rev. 11/13) Search and Seizure Warrant

Special Agent:

Julia MacBeth (FBI)

Telephone: (313) 965-1373

UNITED STATES DISTRICT COURT

for the
Eastern District of MichiganIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)44135 Trent Dr., Clinton Township, Michigan 48038
(More fully described in Attachment A)

Case No. 23-mc-50730-4

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See ATTACHMENT B, violations of:

YOU ARE COMMANDED to execute this warrant on or before July 06, 2023 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .Date and time issued: June 22, 2023 4:41 pm
Judge's signatureCity and state: Detroit, MichiganHon. Elizabeth A. Stafford U. S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

23-mc-50730-4

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title